RECEIVED
CENTRAL FAX CENTER

NOV 15 2004

Yee & Associates, P.C.

4100 Alpha Road
Suite 1100
Dallas, Texas 75244

Main No. (972) 385-8777
Facsimile (972) 385-7766

Facsimile Cover Sheet

To: Commissioner for Patents for **Examiner Vernal U. Brown** **Group Art Unit 2635**	Facsimile No.: **703/872-9306**
From: Carrie Parker Legal Assistant to Wayne P. Bailey	No. of Pages Including Cover Sheet: **49**
Message: Enclosed herewith: • Transmittal Document; and • Appeal Brief.	
Re: Application No. **09/717,521** Attorney Docket No: **AUS9-2000-0560-US1**	
Date: Monday, November 15, 2004	

Please contact us at (972) 385-8777 if you do not receive all pages indicated above or experience any difficulty in receiving this facsimile.	*This Facsimile is intended only for the use of the addressee and, if the addressee is a client or their agent, contains privileged and confidential information. If you are not the intended recipient of this facsimile, you have received this facsimile inadvertently and in error. Any review, dissemination, distribution, or copying is strictly prohibited. If you received this facsimile in error, please notify us by telephone and return the facsimile to us immediately.*

PLEASE CONFIRM RECEIPT OF THIS TRANSMISSION BY FAXING A CONFIRMATION TO 972-385-7766.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Rodriguez et al.**

Serial No.: **09/717,521**

Filed: **November 21, 2000**

For: **Electronic Key System, Apparatus and Method**

§ Group Art Unit: **2635**
§
§ Examiner: **Brown, Vernal U.**
§
§ Attorney Docket No.: **AUS9-2000-0560-US1**
§

35525
PATENT TRADEMARK OFFICE
CUSTOMER NUMBER

Certificate of Transmission Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (703) 872-9306 on November 15, 2004.

By: Carrie Parker
Carrie Parker

TRANSMITTAL DOCUMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:
ENCLOSED HEREWITH:

- Appeal Brief (37 C.F.R. 41.37).

A fee of $340.00 is required for filing an Appellant's Brief. Please charge this fee to IBM Corporation Deposit Account No. 09-0447. No additional fees are believed to be necessary. If, however, any additional fees are required, I authorize the Commissioner to charge these fees which may be required to IBM Corporation Deposit Account No. 09-0447. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No. 09-0447.

Respectfully submitted,

Duke W. Yee
Registration No. 34,285
YEE & ASSOCIATES, P.C.
P.O. Box 802333
Dallas, Texas 75380
(972) 385-8777
ATTORNEY FOR APPLICANTS

RECEIVED
CENTRAL FAX CENTER
NOV 15 2004

Docket No. AUS9-2000-0560-US1 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Rodriguez et al.**

Serial No. **09/717,521**

Filed: **November 21, 2000**

For: **Electronic Key System, Apparatus and Method**

Group Art Unit: **2635**

Examiner: **Brown, Vernal U.**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certificate of Transmission Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (703) 872-9306 on November 15, 2004.

By: Carrie Parker
Carrie Parker

APPEAL BRIEF (37 C.F.R. 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on September 13, 2004.

The fees required under § 41.20(B)(2), and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

RECEIVED
CENTRAL FAX CENTER
NOV 15 2004

Docket No. AUS9-2000-0560-US1 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Rodriguez et al.**

Serial No. **09/717,521**

Filed: **November 21, 2000**

For: **Electronic Key System, Apparatus and Method**

Group Art Unit: **2635**

Examiner: **Brown, Vernal U.**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certificate of Transmission Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (703) 872-9306 on November 15, 2004.

By: Carrie Parker
Carrie Parker

APPEAL BRIEF (37 C.F.R. 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on September 13, 2004.

The fees required under § 41.20(B)(2), and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

REAL PARTY IN INTEREST

The real party in interest in this appeal is the following party: International Business Machines Corporation.

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-78

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: 5 and 33
2. Claims withdrawn from consideration but not canceled: none
3. Claims pending: 1-4, 6-32 and 34-78
4. Claims allowed: none
5. Claims rejected: 1-4, 6-32 and 34-78

C. CLAIMS ON APPEAL

The claims on appeal are: 1-4, 6-32 and 34-78

STATUS OF AMENDMENTS

No amendment after final has been filed for the present application.

SUMMARY OF CLAIMED SUBJECT MATTER

A. CLAIM 1 - INDEPENDENT

Claim 1 is directed to a method for operating an electronic locking device using a wireless communication device. A master key code is received from a master key supplier (Specification page 7, lines 27-29). A secondary key code is generated from the master key code (Specification page 8, lines 3-6). The secondary key code is transmitted to the wireless communication device (Specification page 11, lines 2-16). The secondary key code is also transmitted to the electronic locking device, such that the secondary key code is used by the wireless communication device to operate the electronic locking device in lieu of a by a tangible key (Specification page 10, lines 6-18). The above described method is also described at Specification page 12, line 2 – page 13, line 22 and depicted in the flowchart of Figure 6.

B. CLAIM 15 - INDEPENDENT

Claim 15 is directed to a method of operating an electronic locking device using a wireless communication device. A master key code is received from a master key supplier (Specification page 7, lines 27-29). A secondary key code is generated from the master key code (Specification page 8, lines 3-6), and transmitted to the wireless communication device (Specification page 11, lines 2-16). In addition, a key code is received from the wireless communication device and authenticated based on the secondary key code (Specification page 26, lines 16-21 and page 30, lines 8-11). A command is transmitted to operate the electronic locking device if the key code is authentic (Specification page 30, lines 11-15). The above described method is also depicted in the flowchart of Figures 6 & 7. The key code is essentially used as a mechanism for verifying that the sender of the secondary key code obtained the secondary key code from an authorized key supplier, as described at Specification page 26, lines 21-24.

C. CLAIM 29 – INDEPENDENT (MEANS PLUS FUNCTION)

Claim 29 is a means plus function claim related to Claim 1. The means for receiving a master key code and means for generating a secondary key code are described at Specification page 7, line 27 – page 8, line 2 and page 22, line 7 – page 24, line 9 and shown in Figure 1, elements 104 and 112

and Figure 2, elements 210-240. The first means for transmitting is described at Specification page 11, line 17 - page 12, line 1; page 13, lines 4-22; page 24, lines 10 – 17; and shown in Figure 2, element 250. The second means for transmitting is described at Specification page 12, lines 21 – 32; page 24, lines 18-29; and shown in Figure 2, element 260.

D. CLAIM 30 – INDEPENDENT (MEANS PLUS FUNCTION)

Claim 30 is a means plus function claim. The means for receiving a master key code and means for generating a secondary key code are described at Specification page 7, line 27 – page 8, line 2 and page 22, line 7 – page 24, line 9 and shown in Figure 1, elements 104 and 112 and Figure 2, elements 210-240. The first means for transmitting is described at Specification page 11, line 17 - page 12, line 1; page 13, lines 4-22; page 24, lines 10 – 17; and shown in Figure 2, element 250. Claim 30 also recites specific details of the secondary key code, where the secondary key code includes a secondary key code portion, an activation/expiration portion, a wireless communication device identification portion that identifies the wireless communication device, a time of issue portion, and a time of last use portion, as described at Specification page 26, lines 2-7 and page 26, line 25 – page 28, line 20 and depicted in Figure 4, elements 420-460.

E. CLAIM 43 – INDEPENDENT (MEANS PLUS FUNCTION)

Claim 43 is a means plus function claim related to Claim 15.. The means for receiving a master key code and means for generating a secondary key code are described at Specification page 7, line 27 – page 8, line 2 and page 22, line 7 – page 24, line 9 and shown in Figure 1, elements 104 and 112 and Figure 2, elements 210-240. The first means for transmitting is described at Specification page 11, line 17 - page 12, line 1; page 13, lines 4-22; page 24, lines 10 – 17; and shown in Figure 2, element 250. The means for receiving a key code from the wireless communication device, means for authenticating the key code and means for transmitting a command is described at Specification page 30, lines 3-15 and shown in Figure 1 elements 104 and 112 (the key supplier) and/or elements 106 and 116 (the electronic locking device).

F. CLAIM 56 - INDEPENDENT

Claim 56 is a computer program product claim of similar scope to Claim 1, and thus the concise explanation of the subject matter described above with respect to Claim 1 is equally applicable

here for the concise description of Claim 56.

G. CLAIM 57 - INDEPENDENT

Claim 57 is directed to a method of operating an electronic locking device using a wireless communication device. A secondary key code is requested from a key code supplier (Specification page 12, lines 12-14). A secondary key code associated with the electronic locking device is received, the secondary key code having been generated based on a master key code (Specification page 12, lines 14-20). The received secondary key code is transmitted to the electronic locking device to operate such electronic locking device (Specification page 12, lines 21-32). The above described method is also described at Specification page 28, line 29 – page 29, line 25 and depicted in the flowchart of Figures 5A & 5B.

H. CLAIM 66 – INDEPENDENT (MEANS PLUS FUNCTION)

Claim 66 is a means plus function claim related to Claim 57. The means for requesting a secondary key code from a key code supplier is described at Specification page 12, lines 12-14 and page 28, line 31 – page 29, line 1 and depicted in Figure 1, elements 102 and 114 and Figure 3, elements 310, 330 and 350. The means for receiving the secondary key is described at Specification page 12, lines 14-20 and page 29, lines 1-3 and depicted in Figure 1, elements 102 and 114 and Figure 3, elements 310, 330, 340 and 350. The means for transmitting the received secondary key is described at Specification page 12, lines 21-32 and page 29, lines 8-25 and depicted in Figure 1, elements 102 and 114 and Figure 3, elements 310-350.

I. CLAIM 75 - INDEPENDENT

Claim 75 is a computer program product claim of similar scope to Claim 57, and thus the concise explanation of the subject matter described above with respect to Claim 57 is equally applicable here for the concise description of Claim 75.

J. CLAIM 76 - INDEPENDENT

Claim 76 is directed to a method of operating an electronic locking device using a wireless communication device. A secondary key code for operating the electronic locking device is received from a key supplier (Specification page 10, lines 19-29). A key code is received from

the wireless communication device (Specification page 30, lines 8-9). The key code is authenticated using the secondary key code (Specification page 30, lines 9-11). The electronic lock is operated if the key code is authenticated (Specification page 30, lines 11-13). The above described method is depicted in the flowchart of Figure 7.

K. CLAIM 77 – INDEPENDENT (MEANS PLUS FUNCTION)

Claim 77 is a means plus function claim related to Claim 76. The means for receiving a secondary key code is described at Specification page 10, lines 19-29 and page 12, lines 21-32 and depicted in Figure 1, elements 106 and 116. The means for receiving a key code from a wireless communication device is described at Specification page 30, lines 8-9 depicted in Figure 1, elements 106 and 116. The means for authenticating the key code using the secondary key code is described at Specification page 13, lines 27-28 and page 30, lines 9-11 and depicted in Figure 1, elements 106 and 116. The means for operating the electronic locking device is described at Specification page 13, line 28-30 and page 30, lines 11-13 and depicted in Figure 1, elements 106 and 116.

L. CLAIM 78 - INDEPENDENT

Claim 78 is a computer program product claim of similar scope to Claim 76, and thus the concise explanation of the subject matter described above with respect to Claim 76 is equally applicable here for the concise description of Claim 78.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. GROUND OF REJECTION 1 (Claims 1, 8-11, 14, 15, 18, 20, 22-25, 56, 57, 59, 60-61, 64-66, 68-71, 73, 74, 76 and 77)

Claims 1, 8-11, 14, 15, 18, 20, 22-25, 56, 57, 59, 60-61, 64-66, 68-71, 73, 74, 76 and 77 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Kucharczyk et al. U.S. Patent 6300873.

B. GROUND OF REJECTION 2 (Claims 2, 19, 21, 63, 67 and 72)

Claims 2, 19, 21, 63, 67 and 72 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Kucharczyk et al. U.S. Patent 6570488 in view of Hyatt, Jr. et al. U.S. Patent 5745044.

C. GROUND OF REJECTION 3 (Claims 3-4 and 26-28)

Claims 3-4 and 26-28 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Kucharczyk et al. U.S. Patent 6570488 in view of Bruwer U.S. Patent 6166650 and further in view of Brinkmeyer et al. U.S. Patent 5838251.

D. GROUND OF REJECTION 4 (Claims 6-7)

Claims 6-7 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Kucharczyk et al. U.S. Patent 6570488 in view of Gonzales et al. U.S. Patent 5936544.

E. GROUND OF REJECTION 5 (Claim 12)

Claim 12 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Kucharczyk et al. U.S. Patent 6570488 in view of Henderson et al. U.S. Patent 4947163.

F. GROUND OF REJECTION 6 (Claims 16-17)

Claims 16-17 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Kucharczyk et al. U.S. Patent 6300873 in view of Henry et al. U.S. Patent 5774059.

G. GROUND OF REJECTION 7 (Claims 29, 36-39, 41-43 and 46-53)

Claims 29, 36-39, 41-43 and 46-53 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Waggamon et al. U.S. Patent 6049289 in view of Kucharczyk et al. U.S. Patent 6300873.

H. GROUND OF REJECTION 8 (Claim 30)

Claim 30 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Waggamon et al. U.S. Patent 6049289 in view of Hyatt, Jr. et al. U.S. Patent 5745044.

I. GROUND OF REJECTION 9 (Claims 31-32 and 54-55)

Claims 31-32 and 54-55 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Waggamon et al. U.S. Patent 6049289 in view of Brinkmeyer et al. U.S. Patent 5838251.

J. GROUND OF REJECTION 10 (Claims 34-35)

Claims 34-35 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Waggamon et al. U.S. Patent 6049289 in view of Gonzales et al. U.S. Patent 5936544.

K. GROUND OF REJECTION 11 (Claim 40)

Claim 40 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Waggamon et al. U.S. Patent 6049289 in view of Henderson et al. U.S. Patent 4947163.

L. GROUND OF REJECTION 12 (Claims 44-45)

Claims 44-45 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Waggamon et al. U.S. Patent 6049289 U.S. Patent 6570488 (?) in view of Henry et al. U.S. Patent 5774059.

M. GROUND OF REJECTION 13 (Claim 58)

Claim 58 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Kucharczyk et al. U.S. Patent 6300873 in view of Hyatt, Jr. et al. U.S. Patent 5745044.

ARGUMENT

A. GROUND OF REJECTION 1 (Claims 1, 8-11, 14, 15, 18, 20, 22-25, 56, 57, 59-61, 64-66, 68-71, 73, 74, 76 and 77)

A.1. Claims 1, 8-11, 14, 20, 22, 23

Claim 1 (and similarly for Claims 8-11, 14, 20, 22 and 23) recites that the same key code (secondary key code) is transmitted to both the wireless communication device and the electronic locking device as a part of the synergistic combination of steps recited as a unified method for operating an electronic device using a wireless communication device. This secondary key code is generated from a master key code, and the master key code is received from a master key supplier.

In rejecting Claim 1, the Examiner states that the cited Kucharczyk reference teaches a method of providing an access code (secondary code) generated from a unique seed (master code) received by the server. The Examiner goes on to state that the cited reference also teaches transmitting the access code to the user and delivering the access code to the locking device. As Appellants will show in detail below, the details of how the secondary key code is generated per Claim 1 is different than what is taught by the cited reference, and will also show that the Examiner is improperly using 'snippets' of teachings from alternate embodiments to establish all steps are taught by the cited reference, even though such 'snippet' teachings are for different ways/embodiments to accomplish something and do not co-act together in a uniform fashion.

First, the cited reference does not teach generating a secondary key code from a master key code, where the master key code is received from a master key supplier. The Examiner appears to be reading Kucharczyk's server as reading on the master key supplier; and Kucharczyk's access code as reading on the claimed secondary code. Per such an interpretation, there is no "receiving" of a master key code from a master key supplier as the server uses a unique seed. This unique seed is not 'received'. While such difference may not seem to be of much import – it actually is in that something other than the master key supplier (server) is being used to generate the secondary key, per Claim 1, in that the master key code is received *from* a master key supplier, and a secondary key code is generated from *this* (received) master key code. This can be seen in the preferred embodiment shown in Figure 1, where the key supplier is

different from the master key supplier, and receives a master key code from such master key supplier. Per the Examiner's interpretation of the cited reference, the server itself (the master key supplier, per the Examiner) generates a secondary key code – which is different from what is recited in Claim 1.

Also of significance is that these codes are generated/stored in the electronic device at the time of manufacture (column 7, lines 54-59), with a replica/copy of the codes being maintained in a server. Thus, even then there is no step of receiving a master key code from a master key supplier and generating a secondary key code from this (received) master key code, as expressly recited in Claim 1.

Secondly, the Examiner is using one embodiment described in the reference as reading on part of the claim, and another embodiment to read on the remaining claim features. In particular, in one embodiment Kucharczyk teaches a server providing an access code *to a delivery service* via an internet connection such that the delivery service can use the access code to gain entry to a locked delivery box. The delivery box access codes are pre-stored at manufacture (Col. 7, lines 43-65). *In an alternate embodiment*, access codes are issued sequentially to the delivery service, where a new access code is not issued until the previously issued access code has been used. This embodiment still uses pre-stored access codes within the locking device, as the reference states in describing another feature of this particular embodiment that once all available access codes have been used, the locking device may be initialized with a new set of access codes or the access codes may be recycled (Col. 8, lines 45-48).

Perhaps more germane to the present claim, the cited reference also describes an alternate technique for delivering access codes, where the server 'pushes' access codes to a locking device (Col. 9, lines 15-33). However, in this embodiment, the delivery service provides a tracking number of the package to be delivered to the server, who then pushes this same tracking number to the locking device to be used as the key code. In this embodiment, there is no transmission of a generated key code to both a wireless device and locking device, as the service provider (who will be subsequently using an access code to gain entry to the locking device) already has the access code (the tracking number) which they themselves provided to the server, where the server 'pushes' such code to the locking device. Thus, there is no teaching of transmitting a generated access code to *both* a wireless device *and* a locking device, as claimed.

Another error regarding the rejection of Claim 1 pertains to the claimed wireless communication device itself, where the secondary key code (which is transmitted to both the wireless communication device and locking device, per Claim 1) is used by the wireless communication device to operate the electronic lock. The Examiner cites the wireless link shown in FIG 7 of the cited reference as reading on this wireless device. However, this wireless device is used by the owner/user of the lock itself to exchange information with the server (Col. 13, lines 6-10). While this remote access device may also be used by the owner to unlock to the lock itself without manually entering an access code (Col. 4, lines 36-56), the setting of this access code is manually provided by the owner of the lock and uploaded to a server (Col. 9, lines 34-44). There is no teaching of generating a secondary key code from a master key code and transmitting this secondary key code to this owner-operated wireless communication device.

Thus, it has been shown that Claim 1 is not anticipated by the cited reference, as every element of the claimed invention is not identically shown in a single reference[1].

A.2. Claim 15, 18, 24

With respect to Claim 15 (and similarly for Claims 18 and 24), Appellants urge that the cited reference does not teach generating a secondary key code from a master key code received from a master key supplier, for reasons articulated above with respect to Claim 1.

Still further with respect to Claim 15 (and similarly for Claims 18 and 24), Appellants urge that the cited reference does not teach the claimed features associated with the wireless communication device itself. Per Claim 15, a secondary key code is transmitted to the wireless communication device, and is used by the wireless communication device to operate the electronic locking device. *In addition*, a key code is received from this same wireless communication device, and this key code is authenticated based on the secondary key code. In rejecting Claim 15, the Examiner merely alleges that the cited reference teaches receiving a key code for operating the lock from a remote control unit at column 10, lines 65-67, which according to the Examiner implies authentication of the code in order to operate the lock. Even if such assertion is true, it does not establish that such authentication of the key code *is based*

[1] For a prior art reference to anticipate in terms of 35 U.S.C. 102, every element of the claimed invention must be identically shown in a single reference. *In re Bond*, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990).

upon the secondary key code, as expressly recited in Claim 15.

Further, there is no teaching of the claimed step of "transmitting a command to operate the electronic locking device is the key code is authentic", nor has the Examiner alleged any such teaching.

Thus, Claim 15 is shown to have numerous steps/features not taught by the cited reference. As every claimed element is not identically shown in a single reference, it is shown that Claim 15 has been erroneously rejected under 35 USC 102.

A.3. Claim 25

With respect to Claim 25, Appellants show that the cited reference does not teach the claimed feature of wherein the master key code is received via at least one network, and wherein the at least one network is the Internet. In rejecting Claim 25, the Examiner cites Kucharczyk et al figure 5 as teaching this claimed feature. While Figure 5 does show an internet connection, Appellants urge that there is no teaching of use of such internet connection *to receive a master key code*, for which a secondary key code is generated from, as claimed in Claim 25 (in combination with Claims 1 and 3, of which Claim 25 depends upon). Per the Examiner's own interpretation of the cited reference when rejecting Claim 1, the server itself generates a key code (the alleged secondary key code) from a unique seed (the alleged master code), so there would be no reason to transmit the master key code (the seed) from the server 30 across/on the internet 38 shown in Kucharczyk's Figure 5. Thus, Claim 25 has been erroneously rejected under 35 USC 102 as every claimed element is not identically shown in a single reference.

A.4. Claim 56

With respect to Claim 56, Appellants show that the cited reference does not teach the claimed feature of "third instructions for transmitting the secondary key code to the *wireless communication device*" (emphasis added by Appellants), wherein the secondary key code is transmitted from such wireless communication device to the electronic locking device to operate the electronic locking device. The Examiner states that Kucharczyk et al. teaches "transmitting the secondary key code to the electronic locking device, wherein the electronic locking device is operated in response to receiving the secondary key (col. 4, lines 38-50)" (emphasis added by Appellants). Appellants show that this assertion does not establish anticipation with respect to

Claim 56. Claim 56 recites both an electronic locking device AND a wireless communication device. Of particular noteworthiness is the fact that Claim 56 recites that the secondary code is transmitted to the wireless communication device, whereas the Examiner's assertion regarding the teaching of the cited reference is that the secondary code is transmitted to the electronic locking device. Thus, even assuming arguendo that the Examiner's assertion is true, such assertion does not establish a teaching of the claimed element of "third instructions for transmitting the secondary key code to the wireless communication device, wherein the secondary key code is used by the wireless communication device to operate the electronic locking device". The Examiner's reasoning in rejecting Claim 56 makes no mention of the particular uses of a wireless communication device as expressly recited in Claim 56, and thus has failed to establish, or even allege, a teaching of all claimed elements recited in Claim 56.

This claimed feature advantageously allows for transmitting the key to the wireless communication device such that it can subsequently be used by the wireless communication device to operate the electronic locking device. The cited reference does not teach such an intervening device (wireless communication device) that a key code is transmitted to. Thus, Claim 56 is shown to have been erroneously rejected under 35 U.S.C. § 102(e).

A.5. Claim 57, 59-61, 64-66, 68-71, 73, 74

With respect to Claim 57 (and similarly for Claims 59-61, 64-66, 68-71, 73 and 74), Appellants show that the cited reference does not teach *both receiving and transmitting* of a secondary key code, as claimed. As to the claimed step of receiving the secondary key code, the Examiner cites Kucharczyk et al. col. 5, lines 14-15. This passage states "A bar code entry unit is positioned on storage device 10 (e.g., in place of or in addition to access code entry unit 16) and is configured to pass the access code information included in the modulated laser beam to a computer/controller unit of the access code entry unit". It thus appears that the phrase "to pass the access code information included in the modulated laser beam to a computer/controller unit of the access code entry unit" is being interpreted to read on the claimed "receiving the secondary key code". However, as can be seen, since this access code has now been passed to the access code entry unit, there is no need for further transmission of such code (it has already fulfilled its purpose by being passed to the access code entry unit). So, there is no teaching of then transmitting this received secondary code, as claimed. The passage cited by the Examiner as

reading on such transmitting step (Kucharczyk et al. col. 4, lines 38-50) merely teaches an alternate method of getting an access code into the access code entry unit. There is no teaching of both receiving AND transmitting an access code in cooperative fashion as recited in Claim 57. Therefore, Claim 57 is shown to not be anticipated by the cited reference.

A.6. Claim 76, 77

With respect to Claim 76 (and similarly for Claim 77), Appellants show that the cited reference does not teach the claimed steps of (i) "receiving, from a key supplier, a secondary key code for operating the electronic locking device, the secondary key code having been generated based on a master key code"; (ii) "receiving a key code from the wireless communication device"; (iii) "authenticating the key code using the secondary key code"; and (iv) "operating the electronic locking device if the key code is authenticated". In rejecting Claim 76, the Examiner states that the cited reference teaches three steps of "requesting a secondary key code...", "receiving the secondary key code...", and "transmitting the secondary key code" (see Office Action dated 6/15/2004, bottom of page 6 extending to the top of page 7). However, Appellants show that Claim 76 recites four steps, including a step of authenticating the key code using the secondary key code. The Examiner has not alleged, and the cited reference does not teach, such authentication step. Specifically, the cited reference does not teach receiving of two different codes (a secondary key code and a key code) from two different sources (a key supplier and a wireless communication device), and authenticating one of the codes (the key code) using the other code (the secondary key code). Thus, Claim 76 (and similarly for Claim 77) is shown to have been erroneously rejected as every element of the claimed invention is not shown in a single reference.

B. GROUND OF REJECTION 2 (Claims 2, 19, 21, 63, 67 and 72)

B.1. Claim 2, 21

With respect to Claim 2 (and similarly for Claim 21), Appellants show that none of the cited references teach a secondary key code (which is transmitted to the electronic locking device) that includes a wireless communication device identification portion (for which the secondary key code is transmitted to). In rejecting Claim 2, the Examiner states that Kucharczyk

in view of Bruwer teaches a device identification portion associated to the secondary code, citing col. 10, lines 45-48. Applicants show twofold error in such assertion.

First, the Examiner is improperly using a reference (Bruwer) which is not explicitly identified as being a reference of record for which the 35 USC 103 rejection is based. The Examiner rejects Claim 2 under 35 USC 103 over Kucharczyk in view of Hyatt, and yet in the detailed discussion introduces a third reference (Bruwer) of unknown origin. Thus, the Examiner is improperly using uncited and unknown references in rejecting Claim 2 under 35 USC 103.

Secondly, the alleged identification portion per column 10, lines 45-48 does not identify a wireless communication device, as expressly recited in Claim 2. Rather, such identification is with respect to a storage device (a storage device serial number) which has no wireless functionality. Hyatt's identification portion, as cited by the Examiner at col. 4, lines 52-59 is with respect to codes stored in an EEPROM, and is not a part of a secondary key code that is transmitted to both a wireless communication device and an electronic locking device, as expressly recited in Claim 2. Thus, Claim 2 is shown to have been erroneously rejected as a prima facie case of obviousness has not been established by the Examiner[2].

The features of Claim 2 advantageously provide for identification of an authorized wireless communication device for sending the secondary key code. For example, when the secondary key code is transmitted by the wireless communication device, the wireless communication device may also transmit a device identifier that is then compared to the device identifier encoded in the secondary key code. The electronic locking device will be operated if the two identifiers match. In this way, third parties that may have copied the secondary key code from the authorized wireless communication device will not be able to operate the electronic locking device (Specification page 26, line 31 – page 27, line 16).

B.2. Claim 19

[2] In rejecting claims under 35 U.S.C. Section 103, the examiner bears the initial burden of presenting a prima facie case of obviousness. *In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). Only if that burden is met, does the burden of coming forward with evidence or argument shift to the applicant. Id. "A prima facie case of obviousness is established when the teachings from the prior art itself would appear to have suggested the claimed subject matter to a person of ordinary skill in the art." *In re Bell*, 991 F.2d 781, 782, 26 USPQ2d 1529, 1531 (Fed. Cir. 1993) (quoting *In re Rinehart*, 531 F.2d 1048, 1051, 189 USPQ 143, 147 (CCPA 1976)). If the examiner fails to establish a prima facie case, the rejection is improper and will be overturned. *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988).

As to Claim 19, Appellants urge that none of the cited references teach or suggest the claimed steps identified above regarding the improper rejection of Claim 15 (of which Claim 19 ultimately depends upon, and thus incorporates by reference thereto). Thus, a prima facie case of obviousness has not been established with respect to Claim 19, and such claim is thus shown to have been erroneously rejected under 35 USC 103.

Appellants also show that the Examiner is improperly using a reference (Bruwer) which is not explicitly identified as being a reference of record for which the 35 USC 103 rejection is based. The Examiner rejects Claim 19 under 35 USC 103 over Kucharczyk in view of Hyatt, and yet in the detailed discussion introduces a third reference (Bruwer) of unknown origin. Thus, the Examiner is improperly using uncited and unknown references in rejecting Claim 19 under 35 USC 103.

B.3. Claim 63

As to Claim 63, Appellants urge that none of the cited references teach or suggest the claimed features recited in Claim 58 (of which Claim 63 depends upon, and thus incorporates by reference thereto) - specifically, a secondary key code that includes a secondary key code portion and a wireless communication device identification portion that identifies the wireless communication device. Nor has the Examiner alleged any such teaching or suggestion in rejecting Claim 63. Thus, a prima facie case of obviousness has not been established with respect to Claim 63, and such claim is thus shown to have been erroneously rejected under 35 USC 103.

B.4. Claims 67, 72

As to Claim 67 (and similarly for Claim 72), Appellants urge that none of the cited references teach or suggest the claimed steps identified above regarding the improper rejection of Claim 66 (of which Claim 67 depends upon, and thus incorporates by reference thereto). Thus, a prima facie case of obviousness has not been established with respect to Claim 67, and such claim is thus shown to have been erroneously rejected under 35 USC 103.

Appellants further traverse the rejection of Claim 67 by showing that none of the cited references teach or suggest a secondary key code that includes a secondary key code portion and at least a portion of the master key code of which the generation of the secondary key code was

based upon. Nor has the Examiner alleged any such teaching or suggestion. Thus, Claim 67 is further shown to not be obvious in view of the cited references, as a prima facie case of obviousness has not been established by the Examiner.

C. GROUND OF REJECTION 3 (Claims 3-4 and 26-28)

C.1. Claims 3-4, 26-28

As to Claims 3-4 (and similarly for Claims 26-28), Appellants urge that none of the cited refcrences teach or suggest the claimed steps identified above regarding the improper rejection of Claim 1 (of which Claims 3-4 depend upon, and thus incorporate by reference thereto). Thus, a prima facie case of obviousness has not been established with respect to Claims 3-4 (and similarly for Claims 26-28), and such claims are thus shown to have been erroneously rejected under 35 USC 103.

D. GROUND OF REJECTION 4 (Claims 6-7)

D.1. Claims 6-7

As to Claims 6-7, Appellants urge that none of the cited references teach or suggest the claimed steps identified above regarding the improper rejection of Claim 1 (of which Claims 6-7 depend upon, and thus incorporate by reference thereto). Thus, a prima facie case of obviousness has not been established with respect to Claims 6-7, and such claims are thus shown to have been erroneously rejected under 35 USC 103.

E. GROUND OF REJECTION 5 (Claim 12)

E.1. Claim 12

As to Claim 12, Appellants urge that none of the cited references teach or suggest the claimed steps identified above regarding the improper rejection of Claim 1 (of which Claim 12 depends upon, and thus incorporates by reference thereto). Thus, a prima facie case of obviousness has not been established with respect to Claim 12, and such claims are thus shown to have been erroneously rejected under 35 USC 103.

Appellants also show that the Examiner is improperly using a reference (Bruwer) which is not explicitly identified as being a reference of record for which the 35 USC 103 rejection is

based. The Examiner rejects Claim 12 under 35 USC 103 over Kucharczyk in view of Hyatt, and yet in the detailed discussion introduces a third reference (Bruwer) of unknown origin. Thus, the Examiner is improperly using uncited and unknown references in rejecting Claim 12 under 35 USC 103.

F. GROUND OF REJECTION 6 (Claims 16-17)

F.1. Claims 16-17

As to Claims 16-17, Appellants urge that none of the cited references teach or suggest the claimed steps identified above regarding the improper rejection of Claim 15 (of which Claims 16-17 depend upon, and thus incorporate by reference thereto). Thus, a prima facie case of obviousness has not been established with respect to Claims 16-17, and such claims are thus shown to have been erroneously rejected under 35 USC 103.

Appellants also show that the Examiner is improperly using a reference (Bruwer) which is not explicitly identified as being a reference of record for which the 35 USC 103 rejection is based. The Examiner rejects Claims 16 and 17 under 35 USC 103 over Kucharczyk in view of Hyatt, and yet in the detailed discussion introduces a third reference (Bruwer) of unknown origin. Thus, the Examiner is improperly using uncited and unknown references in rejecting Claims 16 and 17 under 35 USC 103.

G. GROUND OF REJECTION 7 (Claims 29, 36-39, 41-43 and 46-53)

G.1. Claims 29, 37-39, 48, 50-51 and 53

Claim 29 (and similarly for Claims 37-39, 48, 50-51 and 53) recites both a wireless communication device and an electronic locking device. A secondary key code, generated from a master key code received from a master key supplier, is transmitted to the wireless communication device and used by the wireless communication device to operate the electronic locking device. In addition, Claim 29 recites a "second means for transmitting the secondary key code to the electronic locking device using at least one of a wired communication link and wireless communication link". The first means for transmitting transmits the secondary key code to the wireless communication device, and the second means for transmitting transmits the secondary key code to the electronic locking device. Thus, Claim 29 recites transmitting the secondary key code to both the wireless communication device AND the electronic locking

device. This is shown in Appellants' preferred embodiment at Figure 1, elements 114 (wireless device) and 116 (electronic locking device), Figure 6 reference number 630 (transmit key code to wireless device), and Figure 5B reference number 565 (transmit key code to electronic locking device). Appellants show that the cited Waggamon passage (Figure 1) only teaches transmission of a code to a single receiver device 42 (Waggamon Col. 4, lines 3-6). To overcome such deficiency in teaching, the Examiner cites Kucharczyk as teaching generating a secondary key code from a master key code and transmitting the master key code to the locking device. However, this does not establish any teaching or suggestion of transmitting the *same generated key* to two different devices – a wireless device and an electronic locking device – as expressly recited in Claim 29. Thus, a prima facie case of obviousness has not been established with respect to Claim 29 (and similarly for Claims 37-39, 48, 50-51 and 53).

G.2. Claim 36

With respect to Claim 36, Appellants initially show error in the rejection of such claim for reasons given above regarding Claim 29 (of which Claim 36 depends upon). Appellants further show error in the rejection of Claim 36 by showing an improper accounting for the claimed wireless communication device. In rejecting Claim 29, the Examiner states that Waggamon's element 42 reads on the claimed wireless communication device (for which a secondary code is transmitted to), and yet in rejecting Claim 36 the Examiner states that Waggamon's element 40 reads on the claimed wireless communication. Since Claim 36 depends upon Claim 29, and thus includes all the claimed features of Claim 29 in addition to the features recited in Claim 36, it is shown to be improper to change to interpretation of the teachings of Waggamon when analyzing Claims 29 and 36. If Waggamon's element 42 is alleged to read on the claimed wireless communication device when rejecting Claim 29, it is improper to change this position when analyzing Claim 36 and say that instead, Waggamon's element 40 reads on the claimed wireless communication device. In addition, there is no secondary key code transmitted to Waggamon's element 40, and thus element 40 does not teach or suggest a first means for transmitting the secondary key code *to* such device 40. Thus, Claim 36 is shown to have been erroneously rejected.

G.3. Claim 41

With respect to Claim 41, Appellants initially show error in such claim rejection for reasons given above regarding Claim 29 (of which Claim 41 depends upon). Appellants further show error in that none of the cited references teach or suggest the claimed feature of "wherein the electronic locking device is preprogrammed to accept the secondary key code". In rejecting Claim 41, the Examiner states that Waggamon teaches this at Col. 6, lines 41-44. Appellants show that there, Waggamon states:

> "During the learn mode, the receiver 42 intercepts the thirty-two bit hopping code and the twenty-four bit serial number from the transmitter 40. The twenty-four bit serial number (received from the transmitter) and the sixty-four bit manufacturer's key (stored in the receiver at the factory) are then used to independently generate a sixty-four bit "secret key" that is identical to the sixty-four bit "secret key" of the particular transmitter."

As can be seen, this passage states that a hopping code and serial number are intercepted by the receiver, which then generates a secret key. The Examiner has previously stated, in rejected Claim 29, the Waggamon's secret key reads on the claimed "secondary key code". Appellants show Waggamon's receiver is not preprogrammed to accept the secret key. Rather, Waggamon teaches that the secret key is independently generated within the receiver, and thus does not accept the secret key, as claimed. Thus, Claim 41 is further shown to have been erroneously rejected.

G.4. Claim 42

With respect to Claim 42, Appellants show error in such rejection by showing that such claim recites "wherein the second means for transmitting the secondary key code to the electronic locking device performs the transmission at a remote time from transmitting the secondary key code to the wireless communication device." As can be seen, this claim recites a second means for transmitting the secondary key code, such code being transmitted to both an electronic locking device and a wireless communication device, and the transmitting to the electronic device is done at a remote time from transmitting to the wireless communication device.

In rejecting Claim 42, the Examiner states that Waggamon's wireless communication device transmits the secondary code to the receiver of the locking device (figure 2) and the key code is decoded and transmitted to the drive mechanism (64) of the lock of the garage door at a different time than when the secondary code was transmitted to the receiver. The Examiner then states that Kucharczyk teaches generating a secondary key code from a master key code and transmitting the access code to the locking device; transmitting the access code to the user; and using a wireless communication device to operate the locking device. The Examiner then acknowledges there is no teaching of transmitting the secondary key code to the locking device at a remote time from the transmitting of the key code to the locking device, and then makes an unsubstantiated statement that one skilled in the art 'recognizes' that transmitting the key code to the locking device prior to transmitting the key code to the wireless device ensures that the locking device has the secondary key code in its memory before the secondary key code is transmitted by the transmitter. However, the Examiner provides no evidentiary or other basis for establishing why this assertion is true. Appellants urge that the fact that a prior art device could be modified so as to produce the claimed device is not a basis for an obviousness rejection unless the prior art suggested the desirability of such a modification. *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984). There is simply no suggestion of any desire for such modification in the cited references.

In any event, Appellants show that even assuming this assertion is true, it does not teach or suggest what is being claimed in Claim 42. Claim 42 recites that a single functional element ("second means for transmitting") transmits the same thing ("secondary key code") to two different functional elements ("electronic locking device" and "wireless communication device. Per the Examiner's assertion, two functional elements are used for transmitting ("wireless communication device transmits the secondary code to the receiver"; receiver decodes and transmits the results of a decoding operation to lock drive mechanism). That is the first difference – the claim uses a single functional element to perform two transmits whereas the cited references use two elements to transmit in a daisy-chain fashion (the first item transmits to the second item, which then transmits to a third item).

Further, Claim 42 recites that the same thing ("secondary key code") gets transmitted to both the wireless communication device and the electronic locking device. What gets transmitted between Waggamon's transmitter (40) and receiver (42) is different from what gets

transmitted between Waggamon's receiver (42) and lock drive mechanism. Specifically, Waggamon transmits a hopping code and serial number from the transmitter to the receiver (Col. 5, lines 50-55; Figure 7a). Neither the hopping code or the serial number are transmitted between the receiver and lock drive mechanism. Rather, the hopping code is decrypted within the receiver, and a series of checks are performed on the decrypted code to determine code validity. If one of the stored secret keys successfully decrypts the received hopping code, the drive mechanism is activated (Waggamon Col. 7, lines 26-56). There is simply no teaching of a second means for transmitting the secondary key code, such code being transmitted to both an electronic locking device and a wireless communication device, and the transmitting to the electronic device is done at a remote time from transmitting to the wireless communication device. Nor does the cited Kucharczyk reference overcome such deficiency in teaching/suggestion. Thus, Claim 42 is shown to have been erroneously rejected under 35 USC 103 as a prima facie case of obviousness has not been properly established by the Examiner.

G.5. Claims 43, 46 and 52

As to Claim 43 (and similarly for Claims 46 and 52), Appellants urge that none of the cited references teach or suggest the claimed steps identified above regarding the improper rejection of Claim 15. Thus, a prima facie case of obviousness has not been established with respect to Claim 43, 46 and 52, and such claims are thus shown to have been erroneously rejected under 35 USC 103.

G.6. Claim 47

With respect to Claim 47, Appellants initially show error in such claim rejection for reasons given above regarding Claim 43 (of which Claim 47 ultimately depends upon). Further with respect to Claim 47, Appellants show that this claim recites a key code table that includes an entry for the electronic locking device, and the entry includes (i) one or more of a valid secondary key code, (ii) activation/expiration information, and (iii) wireless communication device identification information. In rejected Claim 47, the Examiner merely alleges that Waggamon teaches "the entry for the locking device includes device identification information (col. 4, lines 58-59)". Appellants show that Claim 47 recites that the entry includes the items (i), (ii) and (iii) listed above, and this cited Waggamon passage does not teach these three items for an electronic

locking device entry. Rather, this passage merely states "The inputs to the nonlinear function are (a) the unique twenty-four bit "manufacturer key" and the serial number to generate a unique sixty-four bit "secret key" which is stored in the transmitter. This passage does not teach or suggest any type of entry for an electronic locking device, but rather the details of numbers stored in the transmitter (see also Waggamon Figure 3). In addition, there is no teaching of any type of activation/expiration information, as expressly recited in Claim 47. Thus, Claim 47 is further shown to have missing claimed elements, and thus has been erroneously rejected as a proper prima facie showing of obviousness has not been established by the Examiner.

G.7. Claim 49

With respect to Claim 49, Appellants urge that none of the cited references teach or suggest the claimed features recited in Claim 30 (of which Claim 49 depends upon, and thus incorporates by reference thereto) - specifically, a secondary key code that includes a secondary key code portion, an activation/expiration portion, a wireless communication device identification portion that identifies the wireless communication device, a time of issue portion, and a time of last use portion. Nor has the Examiner alleged any such teaching or suggestion in rejecting Claim 49. In rejecting Claim 49, the Examiner merely states that Waggamon teaches encoding of the secondary code at col. 5, lines 10-12. Appellants show that such assertion does not establish a teaching of encoding all the items recited in Claim 49, as listed above. Thus, Claim 49 is shown to have been erroneously rejection as a prima facie case of obviousness has not been established by the Examiner.

H. GROUND OF REJECTION 8 (Claim 30)

H.1. Claim 30

As to Claim 30, Appellants urge that none of the cited references teach or suggest the claimed features identified above regarding the improper rejection of Claim 2. Thus, a prima facie case of obviousness has not been established with respect to Claim 30, and such claim is thus shown to have been erroneously rejected under 35 USC 103.

I. GROUND OF REJECTION 9 (Claims 31-32 and 54-55)

I.1. Claims 31-32 and 54-55

As to Claims 31-32 and 54-55, Appellants urge that none of the cited references teach or suggest the claimed features identified above regarding the improper rejection of Claim 29 (of which Claims 31-32 and 54-55 depend upon, and thus incorporate by reference thereto). Thus, a prima facie case of obviousness has not been established with respect to Claims 31-32 and 54-55, and such claims are thus shown to have been erroneously rejected under 35 USC 103.

J. GROUND OF REJECTION 10 (Claims 34-35)

J.1. Claims 34-35

As to Claims 34-35, Appellants urge that none of the cited references teach or suggest the claimed features identified above regarding the improper rejection of Claim 29 (of which Claims 34-35 depend upon, and thus incorporate by reference thereto). Thus, a prima facie case of obviousness has not been established with respect to Claims 34-35, and such claims are thus shown to have been erroneously rejected under 35 USC 103.

K. GROUND OF REJECTION 11 (Claim 40)

K.1. Claim 40

As to Claim 40, Appellants urge that none of the cited references teach or suggest the claimed features identified above regarding the improper rejection of Claim 29 (of which Claim 40 depends upon, and thus incorporate by reference thereto). Thus, a prima facie case of obviousness has not been established with respect to Claim 40, and such claim is thus shown to have been erroneously rejected under 35 USC 103.

L. GROUND OF REJECTION 12 (Claims 44-45)

L.1. Claims 44-45

As to Claims 44-45, Appellants urge that none of the cited references teach or suggest the claimed features identified above regarding the improper rejection of Claim 43 (of which Claims 44-45 depend upon, and thus incorporate by reference thereto). Thus, a prima facie case of obviousness has not been established with respect to Claims 44-45 , and such claims are thus shown to have been erroneously rejected under 35 USC 103.

M. GROUND OF REJECTION 13 (Claim 58)

M.1. Claim 58

As to Claim 58, Appellants urge that none of the cited references teach or suggest the claimed features identified above regarding the improper rejection of Claim 57 (of which Claim 58 depends upon, and thus incorporates by reference thereto). Thus, a prima facie case of obviousness has not been established with respect to Claim 58, and such claims are thus shown to have been erroneously rejected under 35 USC 103.

Still further with respect to Claim 58, Appellants urge that none of the cited references teach or suggest a secondary key code (which is transmitted to the electronic locking device) that includes a wireless communication device identification portion (for which the secondary key code is transmitted to). In rejecting Claim 58, the Examiner states that Kucharczyk teaches a device identification portion associated to the secondary code, citing col. 10, lines 45-48. Appellants urge that the alleged identification portion per Kucharczyk column 10, lines 45-48 does not identify a wireless communication device, as expressly recited in Claim 58. Rather, such identification is with respect to a storage device (a storage device serial number) which has not wireless functionality. Therefore, the Examiner has failed to establish a prima facie showing of obviousness with respect to Claim 58, and accordingly such claim has been erroneously rejected under 35 U.S.C. 103.

As a final matter, it is shown that the Examiner has provided no statutory basis for the rejection of Claims 13, 62, 75 or 78 even though such claims are listed on the Office Action Summary Page as being finally rejected. As no specific statutory basis has been given by the Examiner for finally rejecting such claims, Appellants urge that such claims have been improperly finally rejected.

In conclusion, Appellants have shown numerous and substantial errors in the Examiner's rejection of all pending claims in this case, and requests that the Board reverse such rejections.

Duke W. Yee
Reg. No. 34,285
Wayne P. Bailey
Reg. No. 34,289
YEE & ASSOCIATES, P.C.
PO Box 802333
Dallas, TX 75380
(972) 385-8777

CLAIMS APPENDIX

The text of the claims involved in the appeal are:

1. A method of operating an electronic locking device using a wireless communication device, comprising:

receiving a master key code from a master key supplier;

generating a secondary key code from the master key code;

transmitting the secondary key code to the wireless communication device; and

transmitting the secondary key code to the electronic locking device, wherein the secondary key code is used by the wireless communication device to operate the electronic locking device in lieu of by a tangible device.

2. The method of claim 1, wherein the secondary key code includes a secondary key code portion, an activation/ expiration portion, a wireless communication device identification portion that identifies the wireless communication device, a time of issue portion, and a time of last use portion.

3. The method of claim 1, wherein the master key code is received via at least one network.

4. The method of claim 1, further comprising:

sending a master key code request to the master key supplier, the master key code request identifying one or more of a key supplier identifier, a product code of the electronic locking device, an electronic certificate, and a password.

6. The method of claim 1, wherein transmitting the secondary key code to the electronic locking device includes transmitting the secondary key code based on a network address of the electronic locking device.

7. The method of claim 1, wherein transmitting the secondary key code to the electronic locking device includes broadcasting the secondary key code along with an identifier of the electronic locking device.

8. The method of claim 1, wherein the wireless communication device is one of a personal digital assistant, a two-way pager, a mobile telephone device, a wireless transmitter, a handheld computer, a laptop computer, and a Bluetooth™ enabled device.

9. The method of claim 1, wherein transmitting the secondary key code to the wireless communication device includes transmitting the secondary key code using at least one of a wireless communication link and a wired communication link.

10. The method of claim 1, wherein transmitting the secondary key code to the wireless communication device includes transmitting the secondary key code as an attachment to an electronic mail message.

11. The method of claim 10, wherein the electronic mail message is sent to the wireless communication device at a remote time from use of the secondary key code to operate the electronic locking device.

12. The method of claim 1, further comprising receiving a confirmation message from the electronic locking device confirming reprogramming of the electronic locking device to accept the secondary key code.

13. The method of claim 1, wherein the electronic locking device is preprogrammed to accept the secondary key code.

14. The method of claim 1, wherein transmitting the secondary key code to the electronic locking device is performed at a remote time from transmitting the secondary key code to the wireless communication device.

15. A method of operating an electronic locking device using a wireless communication device, comprising:

receiving a master key code from a master key supplier;

generating a secondary key code from the master key code;

transmitting the secondary key code to the wireless communication device, wherein the secondary key code is used by the wireless communication device to operate the electronic locking device in lieu of by a tangible device;

receiving a key code from the wireless communication device;

authenticating the key code based on the secondary key code; and

transmitting a command to operate the electronic locking device if the key code is authentic.

16. The method of claim 15, further comprising:

determining if a number of attempts to operate the electronic locking device within a predetermined period of time exceeds a threshold; and

placing the electronic locking device in a safety mode if the number of attempts exceeds the threshold.

17. The method of claim 16, wherein the safety mode is one of a slow down mode and a freeze mode.

18. The method of claim 15, wherein authenticating the key code includes performing a comparison of the key code to information stored in a key code table.

19. The method of claim 18, wherein the key code table includes an entry for the electronic locking device, and wherein the entry includes one or more of a valid secondary key code, activation/expiration information, and wireless communication device identification information.

20. The method of claim 1, wherein the wireless communication device is a wireless communication device owned by a user.

21. The method of claim 2, wherein the secondary key code portion, the activation/expiration portion, the wireless communication device identification portion, the time of issue portion, and the time of last use portion are encoded.

22. The method of claim 1, further comprising maintaining a record of secondary key codes used to access the electronic locking device.

23. The method of claim 1, wherein generating a secondary key code from the master key code includes at least one of using a random number generator, using a key code algorithm, and using one of a plurality of key code generator algorithms chosen in a random or pseudo-random manner.

24. The method of claim 15, wherein authenticating the key code based on the secondary key code includes determining an activation/expiration time of the secondary key code and determining if a current time is within the activation/expiration time.

25. The method of claim 3, wherein the at least one network is the Internet.

26. The method of claim 1, further comprising:

polling the electronic locking device; and

receiving status information from the electronic locking device in response to polling the electronic locking device.

27. The method of claim 26, wherein the status information includes at least one of a current status of the electronic locking device, a time at which operation of the electronic locking device was last attempted, a key code last used to attempt to operate the electronic locking device, and a wireless communication device identifier of a wireless communication device last used to attempt to operate the electronic locking device.

28. The method of claim 26, further comprising operating the electronic locking device based on the received status information.

29. An apparatus for operating an electronic locking device using a wireless communication device, comprising:

means for receiving a master key code from a master key supplier;

means for generating a secondary key code from the master key code; ~~and~~

first means for transmitting the secondary key code to the wireless communication device, wherein the secondary key code is used by the wireless communication device to operate the electronic locking device in lieu of by a tangible device; and

second means for transmitting the secondary key code to the electronic locking device using at least one of a wired communication link and wireless communication link.

30. An apparatus for operating an electronic locking device using a wireless communication device, comprising:

means for receiving a master key code from a master key supplier;

means for generating a secondary key code from the master key code; and

first means for transmitting the secondary key code to the wireless communication device, wherein the secondary key code is used by the wireless communication device to operate the electronic locking device in lieu of by a tangible device, wherein the secondary key code includes a secondary key code portion, an activation/expiration portion, a wireless communication device identification portion that identifies the wircless communication device, a time of issue portion, and a time of last use portion.

31. The apparatus of claim 29, wherein the master key code is received from the master key supplier via at least one network .

32. The apparatus of claim 29, further comprising:

means for sending a master key code request to the master key supplier, the master key code request identifying one or more of a key supplier identifier, a product code of the electronic locking device, an electronic certificate, and a password.

34. The apparatus of claim 29, wherein the second means for transmitting the secondary key code to the electronic locking device includes means for transmitting the secondary key code based on a network address of the electronic locking device.

35. The apparatus of claim 29, wherein the second means for transmitting the secondary key code to the electronic locking device includes means for broadcasting the secondary key code along with an identifier of the electronic locking device.

36. The apparatus of claim 29, wherein the wireless communication device is one of a personal digital assistant, a two-way pager, a mobile telephone device, a wireless transmitter, a handheld computer, a laptop computer, and a Bluetooth™ enabled device.

37. The apparatus of claim 29, wherein the first means for transmitting the secondary key code to the wireless communication device includes means for transmitting the secondary key code using at least one of a wireless communication link and a wired communication link.

38. The apparatus of claim 29, wherein the first means for transmitting the secondary key code to the wireless communication device includes means for transmitting the secondary key code as an attachment to an electronic mail message.

39. The apparatus of claim 38, wherein the electronic mail message is sent to the wireless communication device at a remote time from use of the secondary key code to operate the electronic locking device.

40. The apparatus of claim 29, further comprising means for receiving a confirmation message from the electronic locking device confirming reprogramming of the electronic locking device to accept the secondary key code.

41. The apparatus of claim 29, wherein the electronic locking device is preprogrammed to accept the secondary key code.

42. The apparatus of claim 29, wherein the second means for transmitting the secondary key code to the electronic locking device performs the transmission at a remote time from transmitting the secondary key code to the wireless communication device.

43. An apparatus for operating an electronic locking device using a wireless communication device, comprising:

means for receiving a master key code from a master key supplier;

means for generating a secondary key code from the master key code;

first means for transmitting the secondary key code to the wireless communication device, wherein the secondary key code is used by the wireless communication device to operate the electronic locking device in lieu of by a tangible device;

means for receiving a key code from the wireless communication device;

means for authenticating the key code based on the secondary key code; and

means for transmitting a command to operate the electronic locking device if the key code is authentic.

44. The apparatus of claim 43, further comprising:

means for determining if a number of attempts to operate the electronic locking device within a predetermined period of time exceeds a threshold; and

means for placing the electronic locking device in a safety mode if the number of attempts exceeds the threshold.

45. The apparatus of claim 44, wherein the safety mode is one of a slow down mode and a freeze mode.

46. The apparatus of claim 43, wherein the means for authenticating the key code includes means for performing a comparison of the key code to information stored in a key code table.

47. The apparatus of claim 46, wherein the key code table includes an entry for the electronic locking device, and wherein the entry includes one or more of a valid secondary key code, activation/expiration information, and wireless communication device identification information.

48. The apparatus of claim 29, wherein the wireless communication device is a wireless communication device owned by a user.

49. The apparatus of claim 30, wherein the secondary key code portion and the one or more of a master key code portion, an activation/expiration portion, a wireless communication device identification portion, a time of issue portion, and a time of use portion are encoded.

50. The apparatus of claim 29, further comprising means for maintaining a record of secondary key codes used to access the electronic locking device.

51. The apparatus of claim 29, wherein the means for generating a secondary key code from the master key code includes at least one of using a random number generator, using a key code

algorithm, and using one of a plurality of key code generator algorithms chosen in a random or pseudo-random manner.

52. The apparatus of claim 43, wherein the means for authenticating the key code based on the secondary key code includes determining an activation/expiration time of the secondary key code and determining if a current time is within the activation/expiration time.

53. The apparatus of claim 31, wherein the at least one network is the Internet.

54. The apparatus of claim 29, further comprising:

means for polling the electronic locking device; and

means for receiving status information from the electronic locking device in response to polling the electronic locking device.

55. The apparatus of claim 54, wherein the status information includes at least one of a current status of the electronic locking device, a time at which operation of the electronic locking device was last attempted, a key code last used to attempt to operate the electronic locking device, and a wireless communication device identifier of a wireless communication device last used to attempt to operate the electronic locking device.

56. A computer program product in a computer readable medium for operating an electronic locking device using a wireless communication device, comprising:

first instructions for receiving a master key code from a master key supplier;

second instructions for generating a secondary key code from the master key code; and

third instructions for transmitting the secondary key code to the wireless communication device, wherein the secondary key code is transmitted from the wireless communication device to the electronic locking device to operate the electronic locking device.

57. A method of operating an electronic locking device using a wireless communication device, comprising:

requesting a secondary key code from a key code supplier;

receiving the secondary key code associated with the electronic locking device, the secondary key code having been generated based on a master key code; and

transmitting the received secondary key code to the electronic locking device, wherein the electronic locking device is operated in response to receiving the secondary key code.

58. The method of claim 57, wherein the secondary key code includes a secondary key code portion and a wireless communication device identification portion that identifies the wireless communication device.

59. The method of claim 57, wherein the wireless communication device is one of a personal digital assistant, a two-way pager, a mobile telephone device, a wireless transmitter, a handheld computer, a laptop computer, and a Bluetooth™ enabled device.

60. The method of claim 57, wherein receiving the secondary key code includes receiving the secondary key code as an attachment to an electronic mail message.

61. The method of claim 60, wherein the electronic mail message is received at a remote time from use of the secondary key code to operate the electronic locking device.

62. The method of claim 57, wherein the electronic locking device is preprogrammed to accept the secondary key code.

63. The method of claim 58, wherein the secondary key code portion and the wireless communication device identification portion are encoded.

64. The method of claim 57, further comprising:

determining if a delete command is received; and

deleting the secondary key code from a key storage if a delete command is received.

65. The method of claim 64, wherein the delete command is received from one of a key supplier and the electronic locking device.

66. A wireless communication apparatus for operating an electronic locking device, comprising:

means for requesting a secondary key code from a key code supplier;

means for receiving the secondary key code associated with the electronic locking device, the secondary key code having been generated based on a master key code; and

means for transmitting the received secondary key code to the electronic locking device, wherein the electronic locking device is operated in response to receiving the secondary key code.

67. The wireless communication apparatus of claim 66, wherein the secondary key code includes a secondary key code portion and at least a portion of the master key code.

68. The wireless communication apparatus of claim 66, wherein the wireless communication apparatus is one of a personal digital assistant, a two-way pager, a mobile telephone device, a wireless transmitter, a handheld computer, a laptop computer, and a Bluetooth™ enabled device.

69. The wireless communication apparatus of claim 66, wherein the means for receiving the secondary key code includes means for receiving the secondary key code as an attachment to an electronic mail message.

70. The wireless communication apparatus of claim 69, wherein the electronic mail message is received at a remote time from use of the secondary key code to operate the electronic locking device.

71. The wireless communication apparatus of claim 66, wherein the electronic locking device is preprogrammed to accept the secondary key code.

72. The wireless communication apparatus of claim 67, wherein the secondary key code portion and the master key code portion are encoded.

73. The wireless communication apparatus of claim 66, further comprising:

means for determining if a delete command is received; and

means for deleting the secondary key code from a key storage if a delete command is received.

74. The wireless communication apparatus of claim 73, wherein the delete command is received from one of a key supplier and the electronic locking device.

75. A computer program product in a computer readable medium for operating an electronic locking device, comprising:

first instructions for requesting a secondary key code from a key code supplier;

second instructions for receiving the secondary key code associated with the electronic locking device, the secondary key code having been generated based on a master key code; and

third instructions for transmitting the secondary key code to the electronic locking device, wherein the electronic locking device is operated in response to receiving the secondary key code.

76. A method of operating an electronic locking device using a wireless communication device, comprising:

receiving, from a key supplier, a secondary key code for operating the electronic locking

device, the secondary key code having been generated based on a master key code;

receiving a key code from the wireless communication device;

authenticating the key code using the secondary key code; and

operating the electronic locking device if the key code is authenticated.

77. An electronic locking device comprising:

means for receiving, from a key supplier, a secondary key code for operating the electronic locking device, the secondary key code having been generated based on a master key code;

means for receiving a key code from a wireless communication device;

means for authenticating the key code using the secondary key code; and

means for operating the electronic locking device if the key code is authenticated.

78. A computer program product in a computer readable medium for operating an electronic locking device, comprising:

first instructions for receiving, from a key supplier, a secondary key code for operating the electronic locking device, the secondary key code having been generated based on a master key code;

second instructions for receiving a key code from the wireless communication device;

third instructions for authenticating the key code using the secondary key code; and

fourth instructions for operating the electronic locking device if the key code is authenticated.

EVIDENCE APPENDIX

There is no evidence to be presented.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.